FIPS 201 Evaluation Program - CHUID Reader (Contactless) Test Procedure

Version 2.0.0
June 30, 2006

GSA

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	03/21/06	Document creation.	Limited
Draft	0.1.0	03/21/06	Submitted to GSA for approval.	GSA
Draft	0.1.1	04/20/06	Updated based on feedback from GSA.	Limited
Draft	0.2.0	04/21/06	Submitted to GSA for approval.	GSA
Draft	0.2.1	05/19/06	Updated based on feedback from GSA.	Limited
Draft	0.2.2	05/22/06	Updated based on feedback from GSA.	Limited
Approved	1.0.0	05/23/06	Approved by GSA.	Public
Revision	1.0.1	06/29/06	Updated based on feedback from GSA.	Limited
Revision	1.1.0	06/29/06	Submitted to GSA for approval.	GSA
Approved	2.0.0	06/30/06	Approved by GSA.	Public

Table of Contents

List of Tables

List of Figures

1 Overview

Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

In addition to derived test requirements developed to test conformance to the NIST standard, GSA has established interoperability and performance metrics to further determine product suitability. Vendors whose products and services are deemed to be conformant with NIST standards and the GSA interoperability and performance criteria will be eligible to sell their products and services to the Federal Government.

1.1 Identification

This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the CHUID Reader (Contactless) (henceforth referred to as the Product) against the subset of applicable requirements that need to be electronically tested for this category.

2   Testing Process

As previously mentioned, this document prescribes detailed test steps that need to be executed in order to test the requirements applicable for this category. Please note that conformance to the tests specified in this document will not result in the Product being compliant to the applicable requirements of FIPS 201. The Product must undergo an evaluation using all the evaluation criteria listed for that category prior to being deemed as compliant. Only products and services that have successfully completed the entire Approval Process will be designated as conformant to the Standard. To this effect, this document only provides details for the evaluation using the Lab Test Data Report approval mechanism.

A Lab Engineer follows the steps outlined below in order to test those requirements that have been identified to be electronically tested. The end result is a compilation of the observed behavior of the Product in the Lab Test Data Report.

For this category, there are two potential Laboratory evaluation paths. If PIV Card Reader submitted for evaluation has a Wiegand^{TM} or USB interface, then it will be evaluated as described in section 3.2.

If PIV Card Reader submitted for evaluation uses any other Reader-to-Host interface, the manufacturer will be required to provide all required documentation specified by corresponding approval and test procedures, as well as demonstrate in the Lab, the product's ability to meet the Laboratory requirements described in section 3.1 of this document. The PIV Card Reader must print a test report which shall be used by the Lab as test data, and incorporated in the application package.

Section 3 provides the test procedures that need to be executed for evaluating the Product as conformant to the requirements of FIPS 201.

3 Test Procedure for CHUID Reader (Contactless)

3.1 Requirements

The following table provides a reference to the requirements that need to be electronically tested within the Lab as outlined in the Approval Procedures document for the Product. The different test cases that are used to check compliance to the requirements is also cross-referenced in the table below.

Identifier #	Requirement Description	Source	Test Case #
R-CHU-CL.3	The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.	Card /Card Reader Interoperability Requirements, Section 2.2.1.1	R-CHU-CL-TP.1
R-CHU-CL.4	The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001.	Card /Card Reader Interoperability Requirements, Section 2.2.1.3	R-CHU-CL-TP.1
R-CHU-CL.5	Buffers shall not be readable through the contactless interface more than 10 cm from the reader.	Card /Card Reader Interoperability Requirements, Section 4.2.1.1	R-CHU-CL-TP.2
R-CHU-CL.6	For evaluation purposes, the data format for physical readers shall consist of two parity bits, Agency Code, System Code and Credential Code elements of the FASC-N along with the Expiration Date (YYYYMMDD) from the CHUID as defined by appendix A of NIST SP 800-73. Each element shall be individually formatted as binary numbers and combined to form a 75 bit string as shown in the figure below. Section 5 of the SIA standard defines a 26 bit format that	Card /Card Reader Interoperability Requirements, Section 3.2.3.1	R-CHU-CL-TP.3

	does not meet the requirements outlined in FIPS or its supporting documents and shall not be used.		
	<table><tr><td></td><td>Position</td><td>Length</td></tr><tr><td>Parity Bit P1</td><td>1</td><td>1</td></tr><tr><td>Agency Code</td><td>2-15</td><td>14</td></tr><tr><td>System Code</td><td>16-29</td><td>14</td></tr><tr><td>Credential Code</td><td>30-49</td><td>20</td></tr><tr><td>Expiration Date</td><td>50-74</td><td>25</td></tr><tr><td>Parity Bit P2</td><td>75</td><td>1</td></tr></table> Note: The first parity bit (P1) is even and shall be calculated over the first 37 bits. The second parity bit (P2) is odd and shall be calculated over the last 36 bits.		
R-CHU-CL.12	The authentication attempt shall compare the CHUID expiration date to the current date and determine card expiry.	FIPS 201, Section 6.2.2	R-CHU-CL-TP.3
R-CHU-CL.13	The reader shall be able to parse data elements from the CHUID to authenticate the cardholder.	FIPS 201, Section 6.2.2	R-CHU-CL-TP.4
R-CHU-CL.14	Data received from the reader shall be the data that was written by the lab on each "Golden" test card.	Derived Test Requirement	R-CHU-CL-TP.5

Table 1 - Applicable Requirements

3.2   Test Components

3.2.1   Baseline Configuration

The baseline configuration describes initial state of the Card Reader Test Fixture and its associated components. A Lab Engineer commences execution of this test procedure after performing the necessary updates to the baseline configuration based on the requirements of the test cases described below.

The Card Reader Test Fixture includes the following components as part of its baseline configuration:

1.   The Host System – It includes the workstation and the Test Application software.
2.   Breakout Box – The USB and Serial Communication cables from the breakout box are connected to the Host System.

Figure 1 provides an illustration of the baseline configuration for the Card Reader Test Fixture.
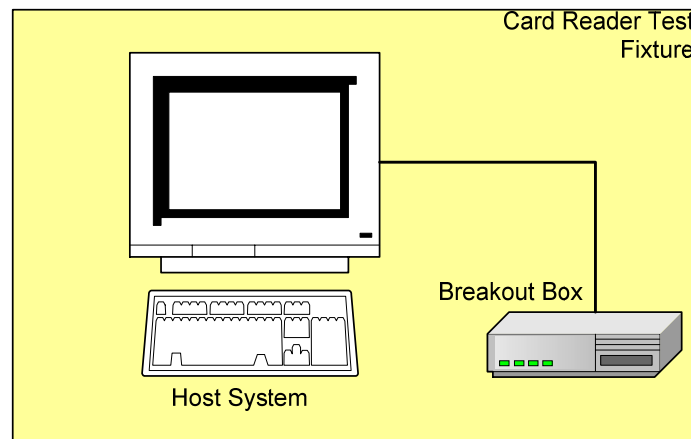
Figure 1 - Card Reader Test Fixture Baseline Configuration

3.2.2   Components Details

Table 2 provides the details of all the components required by the Lab to execute this test procedure. Based on the different test cases, different components may be required to execute the test case.

#	Component	Component Details	Identifier
1	The Card Reader Test Fixture	-	CRTF
2	Contactless PIV Card Reader under test	-	PROD
3	A populated PIV Card that supports the Type A communication signal interface and transmission	Gemplus GemCombi Xpresso R4 E72K PK card with the Gemplus GemPIV applet v1.01	PCARD-A

5

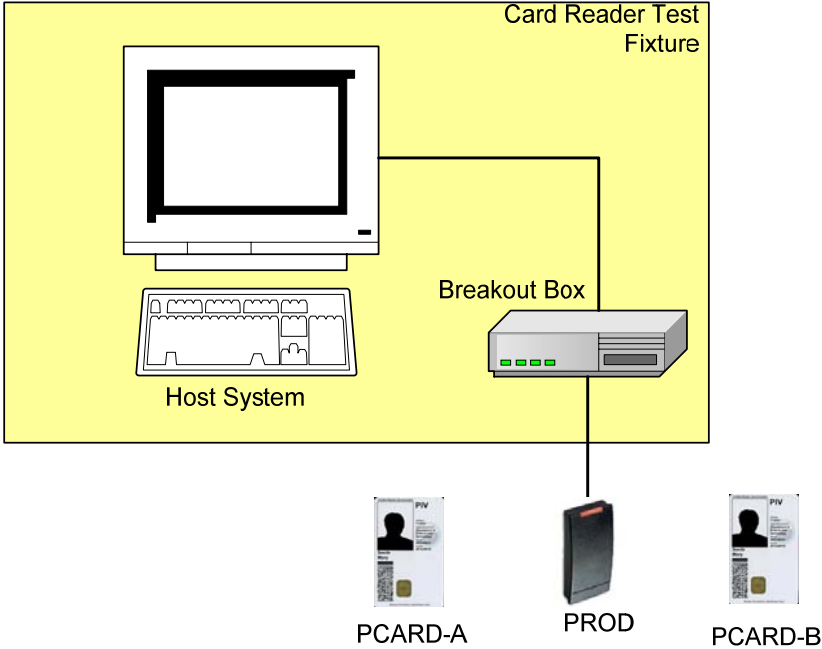| #	Component	Component Details	Identifier
	protocol only.		
4	A populated PIV Card that supports the Type B communication signal interface and transmission protocol only.	TBD	PCARD-B
5	A metric ruler longer than 10 centimeters	-	RULER

Table 2 - Test Procedure: Components

3.3 Test Cases

This section discusses the various test cases that are needed to test the Product against the requirements mentioned above.

3.3.1 Test Case R-CHU-CL-TP.1

3.3.1.1 Purpose

The purpose of this test is to verify that the contactless interface of the reader supports both the Type A and Type B communication signal interfaces and transmission protocols as defined in ISO/IEC 14443-2:2001.

3.3.1.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-A ▪ PCARD-B ▪ PROD ▪ RULER
Configuration Diagram:	 **Figure 2 - Configuration Diagram for Test Case R-CHU-CL-TP.1**
Preparation:	▪ Install the drivers for the PROD in accordance with the manufacturer provided documentation. ▪ Connect the PROD into the appropriate port in the breakout box of the CRTF. ▪ Verify that the PROD is correctly installed by reviewing its

	presence in list of hardware using the device manager of the host system.

3.3.1.3 Test Process

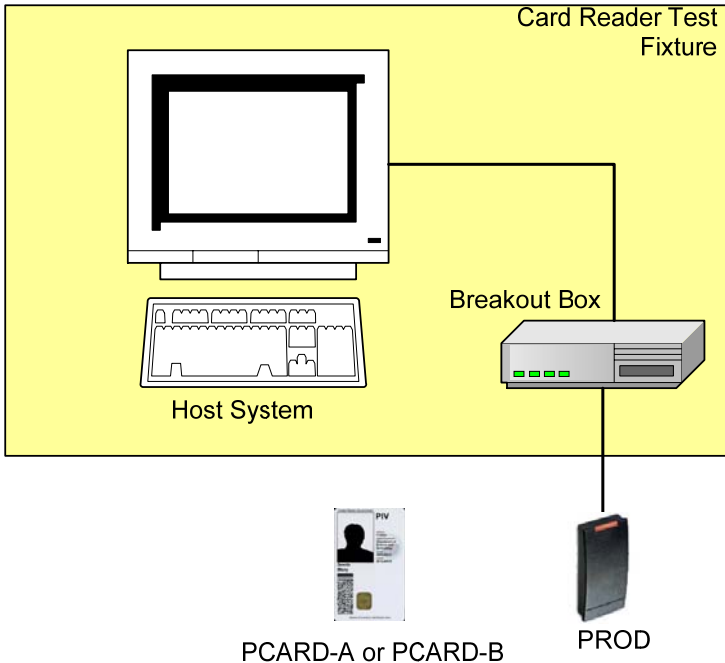|	
Test Steps:	1. Execute the Test Application on the CRTF.
	2. Make sure that the details of the PCARD-A and PCARD-B are entered into the Test Application by in the File → Edit Reference Contactless Card Implementation Info menu bar at the top of the Application window
	3. Select the tab for the "CHUID Reader (Contactless)". This selects the test for the CHUID Reader (Contactless) in the Test Application.
	4. Fill in all the information as required in the screen for the testing the PROD as shown in Figure 6.
	5. Select the Test Case radio button corresponding to R-CHU-CL-TP.1
	6. Bring the PCARD-A within 10 centimeters of the PROD. (Make sure the distance is measured with RULER)
	7. Click on the "Execute Test" button. Follow the steps on the screen.
	8. When prompted, bring the PCARD-B within 10 centimeters of the PROD.
	9. Click the "OK" button to proceed.
	10. Verify that the test was completed by reviewing the result on the screen. (See Figure 10 - Test Report for the CHUID Reader (Contactless).
Expected Result(s):	1. The test completes successfully for both PCARD-A and PCARD-B showing that the CHUID Reader (Contactless) supports both Type A and Type B communication signal interfaces and transmission protocols as defined in ISO/IEC 14443-2:2001 and ISO/IEC 14443-4:2001 respectively.

3.3.2   Test Case R-CHU-CL-TP.2

3.3.2.1 Purpose

The purpose of this test is to verify that the PIV Card buffers shall not be readable through the contactless interface more than 10 cm from the reader.

3.3.2.2 Test Setup

Equipment:	The following components are necessary for executing this test case:
	▪ CRTF
	▪ PCARD-A or PCARD-B
	▪ PROD

	▪ RULER
Configuration Diagram:	Card Reader Test Fixture Breakout Box Host System PCARD-A or PCARD-B PROD **Figure 3 - Configuration Diagram for Test Case R-CHU-CL-TP.2**
Preparation:	▪ No further preparation required in addition to that described in Test Case R-CHU-CL-TP.1

3.3.2.3 Test Process

Test Steps:	1. Select the Test Case radio button corresponding to R-CHU-CL-TP.2 2. Select the radio button for the reference card that is going to be used for this test case. 3. Bring the PCARD-A or PCARD-B within 10 centimeters of the PROD. 4. Click on the "Execute Test" button. Follow the steps on the screen. 5. Verify that the test was completed by reviewing the result on the screen. 6. Once the results have been populated in the Test Results area, click on the "Show Test Report" button. The Test Results screen is displayed. 7. Click on the "Print Report" button to print a copy of the test results for PROD.
Expected Result(s):	1. The test completes successfully for showing that the CHUID Reader (Contactless) is not capable of reading the PIV Card
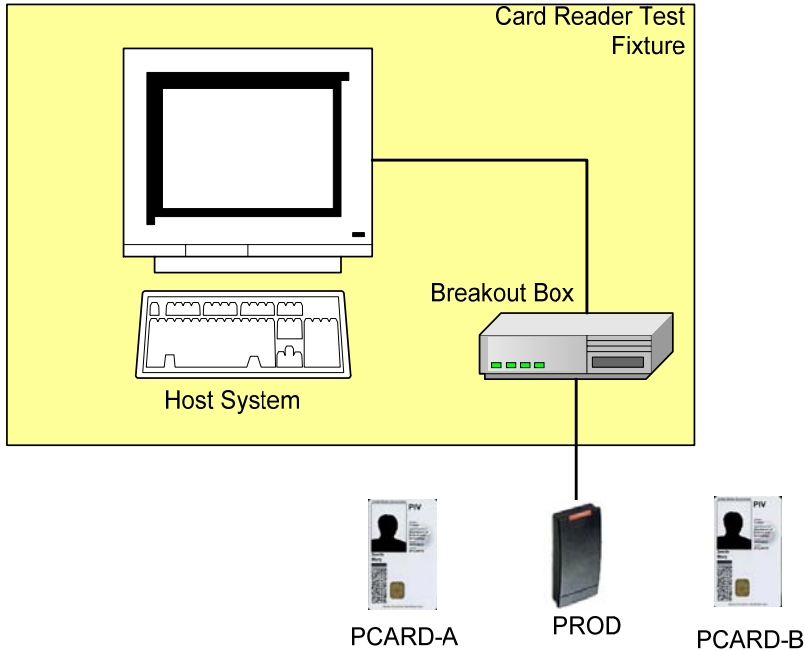
	buffers through the contactless interface when the Card is more than 10 cm from the reader.

3.3.3 Test Case R-CHU-CL-TP.3

3.3.3.1 Purpose

The purpose of this test is to verify that the contactless PIV reader is parsing the correct data elements from the CHUID.

3.3.3.2 Test Setup

Equipment :	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-A ▪ PCARD-B ▪ PROD
Configuration Diagram:	 **Figure 4 - Configuration Diagram for Test Case R-CHU-CL-TP.3**
Preparation:	▪ Generate a new CHUID object and load it onto PCARD-CLA ▪ Load the generated CHUID into the *<configuration file>* for PCARD-A and PCARD-B on the CRTF.

3.3.3.3 Test Process

Test Steps:	1. Select the Test Case radio button corresponding to R-CHU-C-

	TP.3. 2. Make sure that the details of PCARD-T0 and PCARD-T1 are entered into the Test Application by selecting File → Edit Reference Contact Card Implementation Info menu of the top of the Application window (See Figure 9 - Reference Card Information. 3. Insert PCARD-T0 into PROD. 4. Click on the "Execute Test" button. Follow the steps on the screen. 5. Remove PCARD-T0 from PROD. When prompted, insert PCARD-T1. 6. Repeat Step #3 & 4 for PCARD-T1. 7. Verify that the test was completed by reviewing the result on the screen.
Expected Result(s):	1. The test completes successfully showing that the CHUID Reader (Contact) has parsed the correct data elements according to the following table: <table><tr><td></td><td>Position</td><td>Length</td></tr><tr><td>Parity Bit P1</td><td>1</td><td>1</td></tr><tr><td>Agency Code</td><td>2-15</td><td>14</td></tr><tr><td>System Code</td><td>16-29</td><td>14</td></tr><tr><td>Credential Code</td><td>30-49</td><td>20</td></tr><tr><td>Expiration Date</td><td>50-74</td><td>25</td></tr><tr><td>Parity Bit P2</td><td>75</td><td>1</td></tr></table>

3.3.4   Test Case R-CHU-CL-TP.4

3.3.4.1 Purpose

The purpose of this test is to verify that the reader has verified that the PIV Card is not expired.

3.3.4.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-A or PCARD-B ▪ PROD

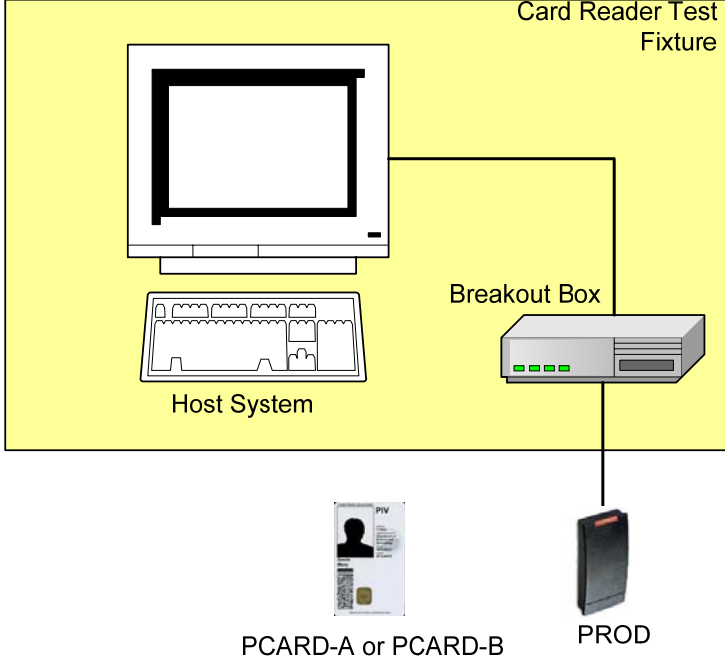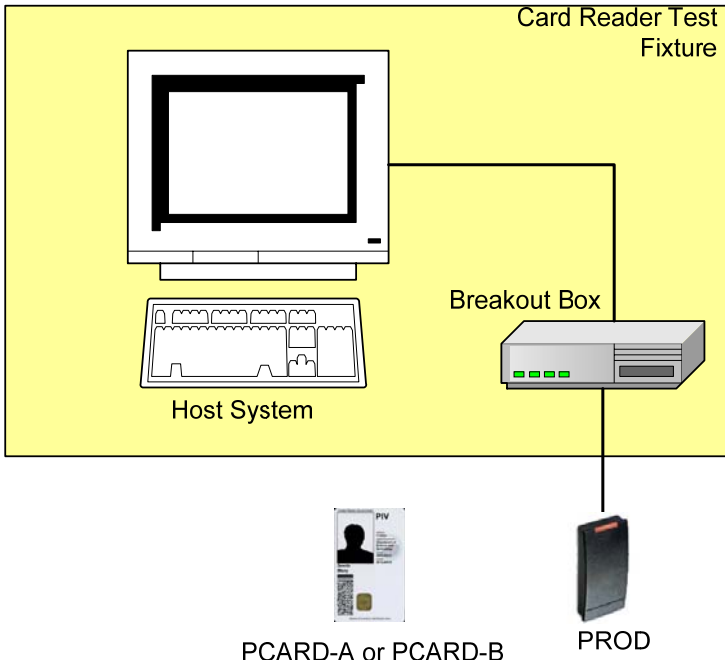| Configuration Diagram:	
	Figure 5 - Configuration Diagram for Test Case R-CHU-CL-TP.4
Preparation:	▪ Check PCARD-A or PCARD-B to ensure that a CHUID exists on the card. If not, generate, if necessary, and load a reference CHUID object which contains an expiration date that is before the current date into the CHUID container on PCARD-A or PCARD-B.

3.3.4.3 Test Process

Test Steps:	1. Select the Test Case radio button corresponding to R-CHU-CL-TP.4
	2. Make sure that the details of card used, PCARD-A or PCARD-B, is entered into the Test Application by selecting File → Edit Reference Contact Card Implementation Info menu of the top of the Application window.
	3. Bring PCARD-A or PCARD-B into proximity with PROD.
	4. Click on the "Execute Test" button. Follow the steps on the screen.
	5. Verify that the test was completed by reviewing the result on the screen. (See Figure 10 - Test Report for the CHUID Reader (Contactless)
Expected Result(s):	1. The test completes successfully showing that the CHUID Reader (Contact) has passed the expected data to the host system.

3.3.5 Test Case R-CHU-CL-TP.5

3.3.5.1 Purpose

The purpose of this test is to verify that the data that is retrieved from the PIV Card has been properly parsed into the proper data elements.

3.3.5.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-A or PCARD-B ▪ PROD
Configuration Diagram:	 **Figure 6 - Configuration Diagram for Test Case R-CHU-CL-TP.5**
Preparation:	▪ Generate some test data that resembles a CHUID object. *Note:* This data must be uniquely generated for each Product submitted for testing. ▪ Load the data into the *<configuration file>* for PCARD-A and PCARD-B.

3.3.5.3 Test Process

Test Steps:	1. Select the Test Case radio button corresponding to R-CHU-CL-TP.5 2. Make sure that the details of PCARD-A and PCARD-B are entered into the Test Application by selecting File → Edit Reference Contact Card Implementation Info menu of the top of

	the Application window. 3. Insert PCARD-A into PROD. 4. Click on the "Execute Test" button. Follow the steps on the screen. 5. When prompted, insert PCARD-B into PROD. 6. Click the "OK" button to proceed. 7. Verify that the test was completed by reviewing the result on the screen. (See Figure 10 - Test Report for the CHUID Reader (Contactless).
Expected Result(s):	1. The test completes successfully showing that the CHUID Reader (Contact) has passed the expected data to the host system.

3.3.6   Test Case R-CHU-CL-TP.6

3.3.6.1 Purpose

The purpose of this test is to verify that the data received through the contact interface of the reader is the data that was expected, and not corrupted during transmission

3.3.6.2 Test Setup

Equipment:	The following components are necessary for executing this test case: ▪ CRTF ▪ PCARD-A ▪ PCARD-B ▪ PROD
Configuration Diagram:	

	Figure 7 - Configuration Diagram for Test Case R-CHU-CL-TP.6
Preparation:	▪ Check PCARD-A to ensure that a CHUID exists on the card. If not, generate, if necessary, and load a reference CHUID object into the CHUID container on PCARD-A and PCARD-B.

3.3.6.3 Test Process

Test Steps:	1. Select the Test Case radio button corresponding to R-CHU-CL-TP.6 2. Make sure that the details of PCARD-A and PCARD-B are entered into the Test Application by selecting File → Edit Reference Contact Card Implementation Info menu of the top of the Application window. 3. Insert PCARD-A into PROD. 4. Click on the "Execute Test" button. Follow the steps on the screen. 5. When prompted, insert PCARD-B into PROD. 6. Click the "OK" button to proceed. 7. Verify that the test was completed by reviewing the result on the screen. (See Figure 10 - Test Report for the CHUID Reader (Contactless).
Expected Result(s):	2. The test completes successfully showing that the CHUID Reader (Contact) has passed the expected data to the host system.

4 CHUID Reader (Contactless) Test Application Screens

4.1 Testing Screen

The following represents a screen shot of the Test Application that is used when testing a CHUID Reader (Contactless). The Lab Engineer is expected to manually provide the information for **CHUID Reader (Contactless) Product Information**, **Tester Information,** and **Test Case Selection** when completing testing.

Figure 8 - Test Screen for the CHUID Reader (Contactless)

4.2   Reference Card Information

The following screen shot depicts the configuration window that will need to be edited to contain the details of the PIV Cards used during testing. Lab Engineers are expected to fill in all fields listed in this window prior to beginning the applicable test.

Figure 9 - Reference Card Information

4.3   Test Report Screen

The following represents a screen shot of the test report that is generated by the Test Application after the CHUID Reader (Contactless) testing has been completed. It provides the Lab Engineer with a reference of what to expect as a result of successful execution of the test procedure. A Lab Engineer is not expected to fill out any portion of the report manually.

Figure 10 - Test Report for the CHUID Reader (Contactless)